

CLAIMS

1 1. A security system for controlling access to a web site from an external
2 network and an internal network, comprising:

3 a security module executing on a security system, the security module for
4 controlling access to web pages;

5 a external web server for servicing requests for web pages from the external
6 network;

7 a site firewall for receiving requests for web pages from the external network
8 and for forwarding legitimate requests for web pages to the external web server;

9 a security firewall for receiving security requests from the external web server
10 and for forwarding legitimate security requests to the security module, the security requests
11 relating to access of a web page; and

12 an internal web server for servicing requests for web pages from the internal
13 network and for forwarding the requests to the security module without passing the requests
14 through the security firewall;

15 whereby requests to access web pages that are received from the external
16 network and the internal network are authorized by the same security module.

1 2. The security system of claim 1 wherein a legitimate request for a web
2 page is an HTTP request.

1 3. The security system of claim 1 wherein a legitimate request for a web
2 page is an HTTPs request.

1 4. The security system of claim 1 wherein the external network is the
2 Internet.

1 5. The security system of claim 1 wherein the external and internal web
2 servers include a module for interfacing to the security module.

1 6. The security system of claim 1 wherein the external and internal web
2 servers implement the same web pages.

1 7. The security system of claim 1 wherein the security module provides
2 authentication services.

1 8. The security system of claim 1 wherein the security module provides
2 authorization services.

1 9. The security system of claim 1 wherein a legitimate security request is
2 received by the security firewall through a designated IP address and port number.

1 10. A method in a computer system for approving access to resources
2 provided by a server, the method comprising:

3 receiving requests to access resources, the requests being received from an
4 external network and an internal network;

5 requesting a security module to approve each request to access a resource
6 irrespective of whether the request was received from the external network or the internal
7 network;

8 when access to the resource is approved, granting access to the requested
9 resource

10 whereby requests to access resource received from either the external network
11 or the internal network are processed by the same security module.

1 11. The method of claim 10 wherein the requests received from the external
2 network are passed through a site firewall before being processed by the server and security
3 requests generated by the server are passed through a security firewall before being
4 processed by the security module.

12. The method of claim 11 wherein the requests received from the internal network are not passed through a site firewall or security firewall.

13. The method of claim 12 wherein the requests received from the external network and requests received from the internal network are processed by different servers.

14. The method of claim 13 wherein the servers are web servers.

15. The method of claim 10 wherein the server is a web server.

16. The method of claim 10 wherein the resources are web pages.

17. The method of claim 10 wherein the external network is the Internet.

18. The method of claim 10 wherein the security module provides authentication services.

19. The method of claim 10 wherein the security module provides authorization services.

20. A security system for controlling access to resources, comprising:
a security module for approving access to the resources;
a server for servicing requests for resources;
a site firewall for receiving requests for resources and for forwarding legitimate requests for resources to the server; and
a security firewall for receiving security requests from the server and for forwarding legitimate security requests to the security module, the security requests relating to approving access to a resource.

21. The security system of claim 20 wherein the requests for resources are received from the Internet.

1 22. The security system of claim 20 wherein a legitimate request for a
2 resource is an HTTP request.

1 23. The security system of claim 20 wherein a legitimate request for a
2 resource is an HTTPs request.

1 24. The security system of claim 20 wherein the requests are received from
2 an external network and wherein requests that are received from an internal network are
3 process by a different server using the same security module, but without using the site
4 firewall or security firewall.

1 25. The security system of claim 20 wherein resources are web pages.

1 26. The security system of claim 20 wherein the security module provides
2 authentication services.

1 27. The security system of claim 20 wherein the security module provides
2 authorization services.

1 28. The security system of claim 20 wherein a legitimate security request is
2 received by the security firewall through a designated IP address and port number.

1 29. A method for configuring computer systems comprising:
2 connecting an external network to a site firewall, the site firewall for receiving
3 requests for web pages from the external network and for forwarding legitimate requests
4 through the site firewall;

5 connecting a external web server to the site firewall, the external web server
6 for servicing legitimate requests for web pages received from the external network;

7 connecting a security firewall to the external web server, the security firewall
8 for receiving security requests from the external web server and for forwarding legitimate
9 security requests;

10 connecting a security module to the security firewall, the security module for
11 receiving legitimate security requests and for approving legitimate security requests;
12 connecting an internal network to an internal web server, the internal web
13 server for servicing requests for web pages received from the internal network; and
14 connecting the security module to the internal web server for receiving security
15 requests and for approving the security requests
16 whereby requests to access web pages that are received from the external
17 network and the internal network are approved by the same security module.

1 30. The method of claim 29 wherein a legitimate request for a web page is
2 an HTTP request.

1 31. The method of claim 29 wherein a legitimate request for a web page is
2 an HTTPs request.

1 32. The method of claim 29 wherein the external network is the Internet.

1 33. The method of claim 29 wherein the external and internal web servers
2 include a module for interfacing to the security module.

1 34. The method of claim 29 wherein the external and internal web servers
2 implement the same web pages.

1 35. The method of claim 29 wherein the security module provides
2 authentication services.

1 36. The method of claim 29 wherein the security module provides
2 authorization services.

1 37. The method of claim 29 wherein a legitimate security request is received
2 by the security firewall through a designated IP address and port number.